Behind the scenes of the VPN Creation Wizard

The new VPN Creation Wizard makes life easier for users that are unfamiliar with the creation of IPsec VPNs. However, not all of the meanings of the fields are intuitive and there are some limitations and requirements that users should be aware of.

Limitations

Types of VPN tunnels

Currently:

- The wizard is only for creating dial up VPN connection tunnels.
- The remote users need one of the following;
  - FortiClient software (version 5)
  - The Cisco client that is included in the Apple iOS software.

Creating Policies

While the wizard does simplify tunnel configuration, such as building both phases 1 and 2 of the tunnel, it does not do everything. For example, policies still have to be created so the tunnel can pass data back and forth.

Requirements

When using the wizard, there are a few pieces of information that you are going to want at your fingertips, or have configured before starting the wizard.

- Know the type of VPN clients are your remote users using.
- If you are using a certificate for authentication, it needs to be installed.
- The User Group that your users belong to. You can create one within the wizard, but it is preferable to take the time to configure it properly before starting the wizard so that there are fewer chances of making mistakes.
- The interface/port to which users will connect.
- Your company's security policy on allowing split tunnel connections to your internal network.

Tour of the VPN Creation Wizard

Section 1 - VPN Setup

Name

Every VPN tunnel needs a unique name that policies can use as a reference. After the tunnel has been completed this name will show up in the drop down menu that lists all of the Interfaces on the FortiGate. The normal best practices approach applies here.

- Don't make the name too long. The field is limited to 15 characters.
- Don't include spaces in the name.

VPN Type

Dial Up - FortiClient Windows, Mac, and Android

Use this option when the remote users will be connecting with the FortiClient software that is installed on their device.

Dial Up - iPhone / iPad Native IPsec Client

Use this option when the remote users will be connecting with the VPN client that is designed by Cisco. While the setting specifically mentions iOS devices, the Cisco VPN client on a Mac also works.

Section 2 - Authentication

Authentication Method

Pre-shared Key

If the Pre-Shared Key option is chosen, the next field will be called Pre-Shared Key. In this case, you could think of it in the same way as a password. It can be a word, a phrase, or even random characters. Just don't make it easy to guess.

RSA Signature

If the RSA Signature option is chosen, the next field will be called Certificate Name. A certificate is more secure than a Pre-Shared Key, but more effort to configure.

User Group

This user group refers to the group to which the users logging into the VPN belong. Each tunnel can only be assigned one user group, so if the users are currently spread across multiple groups or are not part of any group, the options are either to create a group that consists of all the users accessing a single tunnel or to create a tunnel for each of the groups. Remember that everyone in the group will have the credentials to access the tunnel.

Section 3 - Network

Local Outgoing Interface

This will be the interface port on your FortiGate with which you want to associate this tunnel. For instance, if the remote user wants to use the Public IP address used on your WAN port when they are connecting, then that is the interface that gets assigned here.

Address Range

The address range is a pool of IP addresses that will be assigned to any device connecting to the VPN. This range does not have to be a proper subnet range and it can stop and start at any point. For example both 192.168.1.1 - 192.168.1.255 or 192.168.1.3 - 192.168.1.17 would be valid ranges.

These addresses are not assigned to the visiting computers in the way that a DHCP server assigns addresses. These addresses are what the NATed addresses will be. The reason for NATing is that most connections will be from private networks and it is common for people to use standard private IP address ranges. If the remote computer is on a 192.168.1.0 subnet and your network uses the same address range on one of its networks, then the routing could become confusing. Avoid this confusion by assigning remote computers to an address range that you know isn't part of your existing internal network.

Subnet Mask

The subnet mask is for the addresses that are being assigned to the remote devices. By having a subnet, the device knows when it needs to go to a gateway to reach an address.

DNS Server

Use System DNS

The remote device can be assigned the same DNS server that the FortiGate uses.

Specify

The remote device can be assigned a specific DNS server, by IP address. The requirement is that the address be reachable by the computer while connected to the tunnel. If split tunneling is not enabled and the IP address is not reachable from the FortiGate the DNS server will be useless.

Enable IPv4 Split Tunnel

Split tunneling allows the remote computer to use both the VPN connection to the networks controlled by the FortiGate (provided it is allowed by policy) and networks allowed by its regular network connections. If split tunneling were not allowed, all network traffic would have to go through the VPN tunnel. [*Default setting: enabled*]

Accessible Networks

This option defines which addresses the remote computer can access through the FortiGate. The drop down menu lists addresses that have been defined in the FortiGate's Addresses section. When split tunneling is enabled, this can be used to restrict the access to only those network addresses in your network that you want the remote users to access. If split tunneling is disabled, because all of the remote users' traffic goes through the FortiGate, you could also control which sites on the Internet the remote user can access.

Allow Endpoint Registration

When enabled, this setting makes the FortiGate unit send a request to the FortiClient on the remote computer. The FortiGate unit must receive the correct registration key as a response before it can establish the tunnel. To enable and set the registration key on the FortiGate unit go to System > Config > Advanced. [*Default setting: enabled*]

Section 4 - Client Options

The Client Options window only shows up when the FortiClient variation of the Dialup tunnel has been chosen. If the iPhone / iPad version is chosen, only the first three windows of the wizard are available. Because the software at both ends of the connection are written by Fortinet, more detailed information can be communicated back and forth. This gives the administrator more control over the various aspects of the network including those temporary remote nodes that are created when a VPN connection is created. When properly applied, more control can mean more security.

The common factors for all three of these settings are increased convenience for the user and potential security vulnerability. If the computer falls into the control of someone other than its intended user it takes little or no effort to establish a connection.

Save Password

When enabled, this setting allows the FortiClient software on the remote computer to store the password for the user so that it doesn't have to be typed in each time a connection is made. [*Default setting: disabled*]

Auto Connect

When enabled, this setting allows the FortiClient software on the remote computer to be configured so that whenever the FortiClient software is running it will attempt to connect to the VPN tunnel. [*Default setting: disabled*]

Always Up (Keep Alive)

When enabled, this setting allows FortiClient software on the remote computer to keep the connection from timing out due to inactivity. . [*Default setting: disabled*]